Convergence rates for arbitrary statistical moments of random quantum circuits

Winton G. Brown and Lorenza Viola
Department of Physics and Astronomy, Dartmouth College, 6127 Wilder Laboratory, Hanover, NH 03755, USA

We consider a class of random quantum circuits where at each step a gate from a universal set is applied to a random pair of qubits, and determine how quickly averages of arbitrary finite-degree polynomials in the matrix elements of the resulting unitary converge to Haar measure averages. This is accomplished by establishing an exact mapping between the superoperator that describes t-order moments on n qubits and a multilevel $SU(4^t)$ Lipkin-Meshkov-Glick Hamiltonian. For arbitrary fixed t, we find that the spectral gap scales as $1/n$ in the thermodynamic limit. Our results imply that random quantum circuits yield an efficient implementation of ϵ-approximate unitary t-designs.

PACS numbers: 03.67.Ac, 05.30.-d, 05.40.-a

arXiv:0910.0913v3 [quant-ph] 24 Mar 2010

Random quantum states and unitary operators are broadly useful across theoretical physics and applied mathematics. Within quantum information science [1], they play a key role in tasks ranging from quantum data hiding [2] and quantum cryptography [3] to noise estimation in open quantum systems [4–6]. Unfortunately, generating an ensemble of N-dimensional unitary matrices which are evenly distributed according to the invariant Haar measure on $U(N)$ is inefficient, in the sense that the number of required quantum gates grows exponentially with the number of qubits, $n = \log_2 N$ [1]. So-called *unitary t-designs* provide a powerful substitute for Haar-distributed ensembles. Building on the notion of a state t-design [7], a unitary t-design is an ensemble of unitaries whose statistical moments up to order t equal (exactly or approximately) Haar-induced values [6]. That is, a unitary t-design faithfully simulates the Haar measure with respect to any test that uses at most t copies of a selected n-qubit unitary. Ramifications of the theory of t-designs [8] are being uncovered in problems as different as black hole evaporation and fast "scrambling" of information [9], efficient quantum tomography and randomized gate benchmarking [10], quantum channel capacity [11], and the foundations of quantum statistical mechanics [12].

Prompted by the above advances, significant effort has been devoted recently to identifying *efficient* constructions of t-designs and characterizing their convergence properties [2, 6, 13–16]. Harrow and Low established, in particular, the equivalence between approximate 2-designs and *random quantum circuits* as introduced in [4], and conjectured that a random circuit consisting of k=poly(n,t) gates from a two-qubit universal gate set yields an approximate t-design [16]. While supporting numerical evidence was gathered in [17] for low-order moments, and efficient constructions of t-designs were reported in [16] for any $t = \mathcal{O}(n/\log n)$, the extent to which random quantum circuits could be used to implement an approximate t-design for *arbitrary, fixed* t remained open.

In this Letter, we address this question by determining the rate at which, for sufficiently large circuit depth, statistical moments of arbitrary order converge to their limiting Haar values. Our strategy involves two steps: first, for given t, we show that the asymptotic convergence rate is determined by the spectral gap of a certain superoperator, which encapsulates moments up to order t; next, we compute this gap by mapping the t-moment superoperator to a multilevel version of the Lipkin-Meshkov-Glick (LMG) model, which is known to be exactly solvable, and whose low-energy spectrum is well understood in the thermodynamic limit $n \to \infty$ [18]. Our approach ties together t-design theory with established mean-field techniques from many-body physics, extending earlier results by Znidaric [14] for $t = 2$. Furthermore, asymptotic convergence rates allow us to upper bound the convergence time (minimum circuit length, k_c) needed for a desired accuracy ϵ relative to the Haar measure to be reached. For any fixed t, we find that the scaling $k_c \sim n \log(1/\epsilon)$ holds for sufficiently large n and small ϵ.

Moment superoperator.– Let a random quantum circuit of length k be a sequence $U_k \dots U_1$ of k unitary operators on an n-qubit Hilbert space $\mathcal{H} = \otimes_j^n \mathcal{H}_{q_j}$, where each U_i is selected from an ensemble $\{\mu(U), U\}$, for a probability distribution μ with support on a universal gate set. To analyze arbitrary t-order moments, we introduce a Hilbert space $\mathcal{H}_{M_t} = \mathcal{H}^{\otimes 2t}$, which consists of $2t$ copies of $\mathcal{H}$ and we refer to as the *moment space*, with $\dim(\mathcal{H}_{M_t}) \equiv D = N^{2t}$, and a *local moment space* $\mathcal{H}_{l_t}$, which results from grouping factors corresponding to the same qubit in $\mathcal{H}_{M_t}$. That is, $\mathcal{H}_{M_t} = \otimes_j^n \mathcal{H}_{q_j}^{\otimes 2t} = \mathcal{H}_{l_t}^{\otimes n}$, with $\dim(\mathcal{H}_{l_t}) \equiv d = 4^t$. Moments of order t may be described in terms of the following linear operator on $\mathcal{H}_{M_t}$:

$$M_t[\mu] = \int d\mu(U) U^{\otimes t} \otimes U^{*\otimes t} \equiv \int d\mu(U) U^{\otimes t,t}.$$

Physically, $M_t[\mu]$ may be viewed as the *superoperator* induced by the action of t copies of the random circuit on nt-qubit density operators defined on $\mathcal{H}^{\otimes t}$ (see Fig. 1). In line with standard practice in open-system theory [19], we shall introduce "operator kets" in $\mathcal{H}_{M_t}$, denoted $|A\rangle\rangle \equiv A$, and, correspondingly, $\langle\langle A| = A^\dagger$. Thus, a D^2-dimensional operator ket transforms according to $U^{\otimes t,t}|A\rangle\rangle \equiv UAU^\dagger$, under $U \in U(N)$. Once a basis for $\mathcal{H}_{M_t}$ is chosen, the matrix representation of $M_t[\mu]$ specifies a complete set of t-order moments.

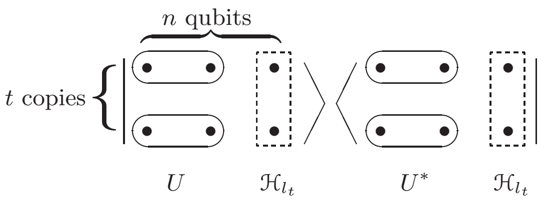

FIG. 1: The moment space $\mathcal{H}_{M_t}$ may be visualized as an array of $2nt$ qubits, in such a way that t copies support a ket in the state space on nt qubits, and the remaining t copies the corresponding bra. In this way, a unitary U on n qubits induces a transformation $U^{\otimes t,t}$ on density operators on nt qubits. Dashed rectangles indicate the $2t$ qubits corresponding to a local moment space $\mathcal{H}_{l_t}$, whereas the ovals correspond to a unitary U acting non-trivially on the first two qubits.

The probability distribution that describes a random circuit of length k, $\mu_k(U)$, is given by the k-th fold convolution of μ with itself [5, 16]. That is, $\mu_k(U) = \int \prod_{i=1}^k d\mu(U_i)\delta(U - \Pi_{i=1}^k U_i)$. It then follows that

$$\begin{aligned} M_t[\mu_k] &= \int \Pi_{i=1}^k d\mu(U_i)\, \Pi_{i=1}^k U_i^{\otimes t,t} \\ &= \prod_{i=1}^k \int d\mu(U_i)\, U_i^{\otimes t,t} = \big(M_t[\mu]\big)^k \equiv M_t^k[\mu]. \end{aligned}$$

Note that, under the assumption that the ensemble $\{\mu(U), U\}$ is invariant under Hermitian conjugation, $\mu(U) = \mu(U^\dagger)$, $M_t[\mu]$ is an Hermitian operator on $\mathcal{H}_{M_t}$.

If $\mu(U)$ has support on a universal set of gates, then the measure over the random circuit converges to the Haar measure on $U(N)$ in the limit of infinite circuit length [5], $\lim_{k\to\infty} \mu_k(U) = \mu_H(U)$. We begin by characterizing how these convergence properties translate in terms of t-order moments. Let $M_t[\mu_H] = \int d\mu_H(U) U^{\otimes t,t}$, and let

$$\mathcal{V}_t = \text{span}\{|\phi\rangle\rangle \in \mathcal{H}_{M_t} \,|\, U^{\otimes t,t}|\phi\rangle\rangle = |\phi\rangle\rangle,\ \forall U \in U(N)\}$$

be the subspace of fixed points of $U^{\otimes t,t}$, $U \in U(N)$, with $\mathcal{P}_{\mathcal{V}_t}$ denoting the corresponding projector. We claim that

$$\lim_{k\to\infty} \big(M_t[\mu]\big)^k = \mathcal{P}_{\mathcal{V}_t} = M_t[\mu_H], \quad \forall t. \tag{1}$$

While this is implied by the results in [16], a self-contained proof follows. Let $|\phi\rangle\rangle$ be an eigenoperator of $M_t[\mu]$ with eigenvalue λ, and $|\phi_U\rangle\rangle \equiv U^{\otimes t,t}|\phi\rangle\rangle$. Since

$$\big|\langle\langle M_t[\mu]\rangle\rangle\big| = \Big|\int d\mu(U)\langle\langle\phi|U^{\otimes t,t}|\phi\rangle\rangle\Big| \le \int d\mu(U)\big|\langle\langle\phi|\phi_U\rangle\rangle\big|,$$

it follows that $|\lambda| \le 1$, with equality holding if and only if $U^{\otimes t,t}|\phi\rangle\rangle = |\phi\rangle\rangle$ for all U with $\mu(U) \neq 0$. Any such operator ket $|\phi\rangle\rangle$ is also invariant under any unitary of the form $U^{\otimes t,t}$, where U is generated by a random circuit of *arbitrary* length, that is, $U = \Pi_{i=1}^k U_i$ for any k, as long as $\mu(U_i) \neq 0$. Thus, if $\mu(U)$ has support on a universal gate set, the eigenspace of eigenvalue 1 is precisely $\mathcal{V}_t$. Since all other eigenvalues of $M_t[\mu]$ have magnitude less than 1, $M_t^k[\mu]$ converges to $\mathcal{P}_{\mathcal{V}_t}$. To establish the second equality in Eq. (1), we invoke the invariance of the Haar measure under $U(N)$, $\mu_H(U) = \mu_H(U'U)$. For $|\phi\rangle\rangle$ an eigenoperator of $M_t[\mu_H]$ with eigenvalue λ, it follows that, $M_t[\mu_H]|\phi\rangle\rangle = \int d\mu_H(U)U^{\otimes t,t}|\phi\rangle\rangle = \lambda|\phi\rangle\rangle$. Thus,

$$\begin{aligned} U'^{\otimes t,t}\lambda|\phi\rangle\rangle &= \int d\mu_H(U)(U'U)^{\otimes t,t}|\phi\rangle\rangle \\ &= \int d\mu_H(U'^\dagger U)U^{\otimes t,t}|\phi\rangle\rangle = \int d\mu_H(U)U^{\otimes t,t}|\phi\rangle\rangle = \lambda|\phi\rangle\rangle. \end{aligned}$$

If $\lambda \neq 0$, it follows that $|\phi\rangle\rangle \in \mathcal{V}_t$, otherwise $\lambda = 0$, which establishes the desired result.

Our next goal is to obtain the *rate* at which $M_t^k[\mu]$ approaches $M_t[\mu_H]$. Since $M_t[\mu_H]$ projects onto the eigenspace of $M_t[\mu]$ of eigenvalue 1, the distance $\|M_t^k[\mu] - M_t[\mu_H]\|$ with respect to any (unitarily invariant) norm depends only on the remaining eigenvalues $\{\lambda_i\}$ of $M_t[\mu]$ and the corresponding eigenprojectors $\{\Pi_i\}$. Specifically, if k is sufficiently large, $\|M_t^k[\mu] - M_t[\mu_H]\| = \Big\|\sum_{\lambda_i\neq 1}\lambda_i^k \Pi_i\Big\| \approx |\lambda_1|^k \|\Pi_1\|$, where $\lambda_1 \equiv 1 - \Delta_t$ is the subdominant eigenvalue of $M_t[\mu]$. Thus, the asymptotic convergence rate is entirely determined by the spectral gap Δ_t of $M_t[\mu]$.

Mean-field solution.– The starting point for mapping $M_t[\mu]$ to an exactly solvable, infinitely-coordinated model is to ensure that the following conditions are obeyed: (i) The applied quantum gates consist only of single- and two- qubit gates selected according to a distribution $\tilde{\mu}(U)$ on $U(4)$, with $\tilde{\mu}(U) = \tilde{\mu}(U^\dagger)$; (ii) The target pair of qubits is picked uniformly at random. We shall generally refer to the class of circuits obeying (i)-(ii) as *permutationally invariant random quantum circuits.* Since, in each application of a random gate U to a fixed pair of qubits, the operator $U^{\otimes t,t}$ acts non-trivially only on the associated bi-local moment space $\mathcal{H}_{l_t} \otimes \mathcal{H}_{l_t}$, and this action is identical for every qubit pair, the moment superoperator for any such circuit may be written as follows:

$$M_t[\mu] = \frac{2}{n(n-1)} \sum_{i<j=1}^n m_t^{ij}[\tilde{\mu}], \tag{2}$$

where for any pair i, j the restriction $m_t[\tilde{\mu}]$ of $m_t^{ij}[\tilde{\mu}]$ to $\mathcal{H}_{l_t} \otimes \mathcal{H}_{l_t}$ acts as $m_t[\tilde{\mu}] = \int d\tilde{\mu}(U)U^{\otimes t,t}$. Recalling that $\dim(\mathcal{H}_{l_t}) = d$, $M_t[\mu]$ thus defines a qu*d*it Hamiltonian, which is invariant under the symmetric group $\mathcal{S}_n$ of permutations of the n local moment spaces. Explicitly, if $\{b^i_{\alpha\beta} = |\alpha\rangle\rangle\langle\langle\beta|\}$ denotes an outer-product basis for operators acting on any $\mathcal{H}_{l_t}$, we may expand $m_t^{ij} = \sum_{\alpha\beta\gamma\delta=1}^d \langle\langle\alpha\gamma|m_t|\beta\delta\rangle\rangle b^i_{\alpha\beta}b^j_{\gamma\delta} \equiv \sum_{\alpha\beta\gamma\delta=1}^d c_{\alpha\beta\gamma\delta}b^i_{\alpha\beta}b^j_{\gamma\delta}$, and rewrite $M_t[\mu]$ as a quadratic function of the collective operators $B_{\alpha\beta} = \sum_{i=1}^n b^i_{\alpha\beta}$, that is, $M_t[\mu] = \frac{1}{n(n-1)}\sum_{\alpha\beta\gamma\delta=1}^d c_{\alpha\beta\gamma\delta}(B_{\alpha\beta}B_{\gamma\delta} - \delta_{\beta\gamma}B_{\alpha\delta})$. Since the operators $B_{\alpha\beta}$ obey $SU(d)$ commutation rules,

$[B_{\alpha\beta}, B_{\gamma\delta}] = B_{\alpha\delta}\delta_{\beta\gamma} - B_{\beta\gamma,}\delta_{\alpha\beta}$, $\mathcal{H}_{M_t}$ carries the (reducible) collective n-fold tensor product representation of $SU(d)$, and $M_t[\mu]$ provides a d-level extension of the standard, spin-1/2 LMG model [20].

Thanks to the invariance under $\mathcal{S}_n$, each of the eigenoperators of $M_t[\mu]$ belongs to an irreducible representation (irrep) of $SU(d)$. Our first step is to show that the eigenspace $\mathcal{V}_t$ of $M_t[\mu]$ corresponding to the ground-state (extremal) eigenvalue of 1 lies in the totally symmetric irrep, of dimension $d_S = \binom{4^t+n-1}{n}$ [21]. Recall that $\mathcal{V}_t$ consists of operators in $\mathcal{H}_{M_t}$ that commute with all t-fold tensor power unitaries $U^{\otimes t}$. By Schur-Weyl duality [16, 21], every such operator is a linear combinations of elements of $\mathcal{S}_t$, under the natural representation in $\mathcal{H}^{\otimes t}$. Note that the operators spanning $\mathcal{V}_t$ are permutations of the t copies of $\mathcal{H}$ rather than permutations of the n local moment spaces $\mathcal{H}_{l_t}$. One may write any such permutation as $|\sigma^{(n)}\rangle\rangle = \sum_{i_1\ldots i_t=1}^{N} |i_1 \ldots i_t\rangle\langle i_{\sigma(1)} \ldots i_{\sigma(t)}|$, where $\sigma \in \mathcal{S}_t$. Furthermore, each such permutation may be viewed as a *product ket* relative to the factorization $\mathcal{H}_{M_t} = \mathcal{H}_{l_t}^{\otimes n}$. Explicitly, $|\sigma^{(n)}\rangle\rangle = \big(|\sigma\rangle\rangle\big)^{\otimes n}$, where $|\sigma\rangle\rangle = \sum_{i_1\ldots i_t=0,1} |i_1 \ldots i_t\rangle\langle i_{\sigma(1)} \ldots i_{\sigma(t)}| \in \mathcal{H}_{l_t}$. The fact that $\mathcal{V}_t$ is *exactly spanned* by product states is significant from the perspective of mean-field theory. For arbitrary $SU(d)$ quadratic Hamiltonians, it has been rigorously established that the exact ground-state energy is given in the thermodynamic limit by a mean-field Ansatz equivalent to assuming that the ground state is an $SU(d)$ coherent state [20]. Since, for the completely symmetric irrep, the manifold of coherent states consists precisely of all product states [22], the mean-field extremal eigenspace of $M_t[\mu]$ is, in fact, *exact for any n.*

The next step is to determine the lowest excitation energy in the large-n limit, which is accomplished by expanding $M_t[\mu]$ around an arbitrary extremal mean-field state for each irrep [24]. While, to our knowledge, a rigorous justification of such a mean-field Ansatz is lacking, its validity for LMG Hamiltonians is supported by an extensive body of theoretical and numerical investigations [18]. For the totally symmetric irrep, the required diagonalization procedure is most straightforwardly carried out by realizing the $U(d)$ algebra in terms of d canonical Schwinger boson operators $\{a_\alpha, a^\dagger_\beta\}$ [23]. That is, we let $B_{\alpha\beta} = a^\dagger_\alpha a_\beta$ and rewrite the LMG Hamiltonian as $M_t[\mu] = \frac{1}{n(n-1)} \sum_{\alpha\beta\gamma\delta=1}^{d} c_{\alpha\beta\gamma\delta} a^\dagger_\alpha a^\dagger_\gamma a_\beta a_\delta$. Since the totally symmetric irrep of $\mathcal{H}_{M_t}$ contains exactly n Schwinger bosons, it is possible to eliminate one boson mode by regarding it as "frozen" in the vacuum for a generalized Holstein-Primakoff transformation [23]. Specifically, let the local basis be chosen so that the frozen mode corresponds to $|\sigma\rangle\rangle$, and let $\theta(n) \equiv (n - \sum_{\alpha\neq\sigma} a^\dagger_\alpha a_\alpha)^{1/2}$, with $a^\dagger_\sigma \to \theta(n)$, $a_\sigma \to \theta(n)$. Two simplifications may now be invoked: first, the fact that $|\sigma^{(n)}\rangle\rangle$ is an exact ground state causes any coefficient of the form $c_{\alpha\sigma\beta\sigma}$, $c_{\alpha\sigma\sigma\sigma}$ (and their complex conjugates) to vanish; second, only terms up to the leading order in $1/n$ need to be kept in $\theta(n)$. This finally yields: $M_t[\mu] = 1 - \frac{1}{n}\sum_{\alpha\beta=1}^{d} E_{\alpha\beta} a^\dagger_\alpha a_\beta + \mathcal{O}(1/n^2)$, where $E_{\alpha\beta} = 2(\delta_{\alpha\beta} - \langle\langle\sigma\alpha|m_t|\sigma\beta\rangle\rangle - \langle\langle\sigma\alpha|m_t|\beta\sigma\rangle\rangle)$. To leading order, the desired gap is then determined by the smallest eigenvalue, a_1, of $E_{\alpha\beta}$. That the latter is *nonzero* may be shown by exploiting basic properties of the superoperator m_t [24]. This establishes our first main result: For any permutationally invariant random quantum circuit, and for any fixed $t > 0$, the spectral gap may be expanded as

$$\Delta_t = \sum_{p=1}^{\infty} a_p n^{-p} = \frac{a_1}{n} + \mathcal{O}\Big(\frac{1}{n^2}\Big), \qquad (3)$$

for coefficients $\{a_p\}$ that may in general depend on t.

A stronger result may be obtained for a sub-class of random quantum circuits which are, in addition, *locally invariant*, that is, $\tilde{\mu}(U)$ is invariant under the subgroup $U(2)\times U(2) \subset U(4)$ of local unitary transformations on the two target qubits. In this case, it is possible to choose a basis for each local moment space $\mathcal{H}_{l_t}$, which includes a maximal set of t-qubit operators $\{|\omega\rangle\rangle\}$ in the commutant of $U^{\otimes t}$, with $U \in U(2)$. Accordingly, every matrix element $\langle\langle\alpha\beta|m_t|\gamma\delta\rangle\rangle = 0$, unless each local basis element is itself an invariant, and the large-n behavior of the gap is determined by matrix elements of the form $\langle\langle\sigma\omega|m_t|\sigma\omega\rangle\rangle$ and $\langle\langle\sigma\omega|m_t|\omega\sigma\rangle\rangle$, with $\sigma \in \mathcal{S}_t$ (without loss of generality, we may choose $|\omega\rangle\rangle = |I\rangle\rangle$) and $|\omega\rangle\rangle$ an arbitrary $U(2)$-invariant with $\langle\langle\sigma|\omega\rangle\rangle = 0$. Since, for $t > 1$, the maximum value of any such matrix element is independent of t (see [24] for full detail), it follows that the leading order term a_1 *does not depend on t* for locally invariant random quantum circuits.

Example.– Consider the simplest case where $t = 2$ and $\tilde{\mu}(U) = \mu_H(U)$ on $U(4)$. The invariant eigenspace $\mathcal{V}_2$ of M_2 is spanned by the identity $|I^{(n)}\rangle\rangle = \big(|I\rangle\rangle\big)^{\otimes n}$ and the permutation $|S^{(n)}\rangle\rangle = \big(|S\rangle\rangle\big)^{\otimes n}$ that swaps the $t = 2$ copies of $\mathcal{H} = \mathcal{H}_q^{\otimes n}$. Since $\tilde{\mu}(U)$ is the Haar measure, m_2 coincides with the projector onto the subspace $\mathcal{V}_2$ for $n = 2$ qubits. An orthogonal basis for $\mathcal{V}_2$ may be formed by taking even/odd linear combinations under swap, $|A_\pm\rangle\rangle = |I^{(2)}\rangle\rangle \pm |S^{(2)}\rangle\rangle$. To find the excitation energies, we choose one of the extremal local kets, $|I\rangle\rangle$, and minimize $E_{\min} = 2\min(1 - \langle\langle I\alpha|m_2|I\alpha\rangle\rangle - \langle\langle I\alpha|m_2|\alpha I\rangle\rangle)$, over all local operators $|\alpha\rangle\rangle \in \mathcal{H}_{l_t}$ orthogonal to $|I\rangle\rangle$. This yields $|\alpha\rangle\rangle = |S\rangle\rangle - \langle\langle S|I\rangle\rangle|I\rangle\rangle = \sigma_1^1\sigma_1^2 + \sigma_2^1\sigma_2^2 + \sigma_3^1\sigma_3^2$, and $\Delta_t = 6/5n + \mathcal{O}(1/n^2)$. To determine how quickly the large-n scaling sets in, the fully symmetric sector of $M_t[\mu]$ under $\mathcal{S}_n$ was numerically diagonalized. Since $\mu_H(U)$ is invariant under $U(2)\times U(2)$ transformations, $\mathcal{H}_{l_2}$ may be restricted to the subspace of $SU(2)$ invariants. From angular momentum theory [21], the number of such invariants is $\sum_J m_J^2 = \frac{(2t)!}{(t+1)!t!} = C_t$, where m_J is the multiplicity of the $SU(2)$-irrep with total angular momentum J. This yields $d_S^{\rm loc} = \binom{C_t+n-1}{n} \ll d_S$, which makes numerical comparisons tractable for small t. Exact results

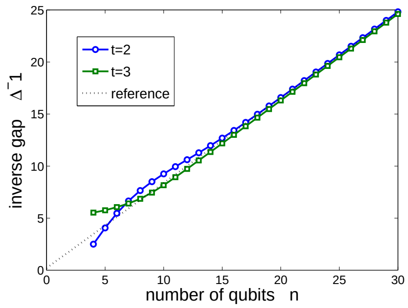

FIG. 2: (Color online) Inverse spectral gap Δ_t^{-1} of $M_t[\mu_H]$ with $t = 2, 3$ for a random circuit consisting of two-qubit gates selected according to the Haar measure on $U(4)$. The line with slope 5/6 corresponds to the asymptotic result.

for t=2 and 3 (see Fig. 2) indicate that the scaling prediction for Δ_t becomes very accurate for $n \gtrsim 14$.

Convergence time.– In order to establish the usefulness of a random circuit as an ϵ-approximate unitary t-design [6, 16], we need to upper-bound the circuit length required to achieve a specified accuracy, ϵ. Let the convergence time with respect to a given norm be defined by the minimum length k_c for which $\|M_t^{k_c}[\mu] - M_t[\mu_H]\| \leq \epsilon$. That $M_t[\mu]$ be operationally indistinguishable from $M_t[\mu_H]$ requires that the supremum of $\|(M_t^k[\mu] - M_t[\mu_H])(\rho)\|_1$ be sufficiently small over all nt-qubit density operators ρ. We may bound the 1-norm starting from the 2-norm [16]. For any density matrix ρ, $\|(M_t^k[\mu] - M_t[\mu_H])(\rho)\|_2 \leq \lambda_1^k$. This follows from normalization of ρ and the fact that $M_t[\mu_H]$ projects onto the eigenspace of eigenvalue 1 of $M_t[\mu]$. In conjunction with the Cauchy-Schwartz inequality, this implies $\|(M_t^k[\mu] - M_t[\mu_H])(\rho)\|_1 \leq 2^{nt}\lambda_1^k$. Requiring that $2^{nt}\lambda_1^{k_c} \leq \epsilon$ finally yields $k_c \leq \Delta_t^{-1}(\log(1/\epsilon) + nt\log(2))$. Since, using Eq. (3), $\Delta_t^{-1} = \sum_{p=1}^{\infty} a'_p n^{2-p} \sim a_1^{-1} n$ to leading order, $k_c = a_1^{-1} n \log(1/\epsilon)$ for sufficiently small ϵ. It is worth stressing that we have *not* addressed how k_c scales at fixed n while letting $t \to \infty$. To answer this question it is necessary to determine how a'_1 depends on t, as well as the minimum value of n required for the linear term $a'_1 n$ to dominate. While this is important for a full characterization of t-designs, our results are directly relevant to physical applications, where t is fixed.

In summary, we have established that a large class of random quantum circuits are efficient ϵ-approximate unitary t-designs for arbitrary finite t. The fact that the extremal eigenoperators are separable suggests that similar results might be established for more general random circuits for which the Hermiticity and the $\mathcal{S}_n$-invariance assumptions of the moment superoperator need not hold [25]. As mentioned, a remaining open question is to determine how the circuit length scales as the limits of large n and large t are taken together. This may resolve the apparent paradox that while Haar random unitaries are inefficient, arbitrary t-designs are not, possibly with equal asymptotic rates. We believe that our findings, along with the techniques introduced to analyze moments of unitary ensembles, will enable further understanding and applications of t-designs across quantum physics.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Information and Quantum Computation* (Cambridge University Press, Cambridge, 2000).

[2] D. P. DiVincenzo, D. W. Leung, and B. Terhal, IEEE Trans. Inf. Theory **48**, 580 (2002).

[3] A. Harrow, P. Hayden, and D. W. Leung, Phys. Rev. Lett. **92**, 187901 (2004); P. Hayden *et al.*, Commun. Math. Phys. **250**, 371 (2004); A. Ambainis and A. Smith, *Lect. Notes Comp. Science* **3122**, 249 (2004).

[4] J. Emerson *et al.*, Science, **302**, 2098 (2003).

[5] J. Emerson, E. Livine, and S. Lloyd, Phys. Rev. A **72**, 060302(R) (2005).

[6] C. Dankert *et al.*, Phys. Rev. A **80**, 012304 (2009).

[7] A. Ambainis and J. Emerson, IEEE Conf. Comp. Complexity **129** (2007).

[8] D. Gross, K. Audenaert, and J. Eisert, J. Math. Phys. **48**, 052104 (2007).

[9] J. Preskill and P. Hayden, J. High Energy Phys. **9**, 120 (2007); Y. Sekino and L. Susskind, *ibid.* **10**, 065 (2008).

[10] A. Bendersky, F. Pastawski, and J. P. Paz, Phys. Rev. A **80**, 032116 (2009); E. Magesan, R. Blume-Kohout, and J. Emerson, arXiv:0910.1315.

[11] M. B. Hastings, Nature Phys. **5**, 255 (2009).

[12] R. A. Low, arXiv:0903.5236.

[13] R. Oliveira, O. C. Dahlsten, and M. B. Plenio, Phys. Rev. Lett. **98**, 130502 (2007); O. C. O. Dahlsten, R. Oliveira, and M. B. Plenio, J. Phys. A **40**, 8081 (2007).

[14] M. Znidaric, Phys. Rev. A **76**, 012318 (2007); *ibid.* **78**, 032324 (2008).

[15] W. G. Brown, Y. S. Weinstein, and L. Viola, Phys. Rev. A **77**, 040303(R) (2008); Y. S. Weinstein, W.G. Brown, and L. Viola, *ibid.* **78**, 052332 (2008).

[16] A. W. Harrow and R. Low, Commun. Math. Phys. **291**, 257 (2009); A. W. Harrow and R. Low, arXiv:0811.2597.

[17] L. Arnaud and D. Braun, Phys. Rev. A **78**, 062329 (2008).

[18] G. Ortiz *et al.*, Nucl. Phys. B **701**, 421 (2005); P. Ribeiro, J. Vidal, and R. Mosseri, Phys. Rev. Lett. **99**, 050402 (2007); S. Dusel and J. Vidal, Phys. Rev. B **71**, 224420 (2005); F. Leyvraz and W. D. Heiss, Phys. Rev. Lett. **95**, 050402 (2005). While the standard two-level LMG model is addressed in these papers, none of the derivations depends specifically on the subsystems' dimension.

[19] R. Alicki and K. Lendi, *Quantum Dynamical Semigroups and Applications* (Springer, Berlin, 1987).

[20] R. Gilmore, J. Math. Phys. **20**, 891 (1979).

[21] J. P. Elliott and P. G. Dawber, *Symmetry in Physics* (Oxford University Press, New York, 1979), Vol. 2.

[22] W. Zhang, D. Feng, and R. Gilmore, Rev. Mod. Phys. **62**, 867 (1990).

[23] S. Okubo, J. Math. Phys. **16**, 528 (1975).

[24] See EPAPS Document No. xxxxxxxx for additional technical details. For more information on EPAPS, see http://www.aip.org/pubservs/epaps.html.

[25] W. G. Brown and L. Viola, in preparation.

Appendix: Supplementary Material

Additional remarks on the determination of the spectral gap

The diagonalization procedure illustrated in the main text determines both the extremal and neighboring eigenvalues of M_t belonging to the totally symmetric irrep of $SU(d)$. Although expressed in terms of bosonic operators, the procedure is equivalent to a variational Ansatz whereby the trial wavefunction of the extremal state is of the form

$$|\phi\rangle\rangle^{\otimes n} = |\phi \dots \phi\rangle\rangle,$$

and the first excited state, corresponding to a single bosonic excitation, is of the form

$$|n_\phi = n-1, n_\alpha{=}1\rangle\rangle \equiv \frac{1}{\sqrt{n}}(|\phi \dots \phi\alpha\rangle\rangle + \dots + |\alpha\phi \dots \phi\rangle\rangle).$$

In principle, it is possible that the subdominant eigenvalue may lie instead in the $SU(d)$ irrep which carries exactly one anti-symmetric pair of indexes (see *e.g.* Ref. [21]). This can be accommodated by using a different variational Ansatz for the excited state to be minimized. If, as in the main text, we choose a local basis in $\mathcal{H}_{\ell_t}$ that includes the fixed extremal permutation $|\sigma\rangle\rangle$, with the remaining local basis operators $|\alpha\rangle\rangle \neq |\sigma\rangle\rangle$ treated as excitation modes, the relevant single-excitation band is spanned by kets of the following form:

$$|n_\sigma = n-1, n_\alpha{=}1\rangle\rangle \equiv \frac{1}{\sqrt{2}}\big(|\sigma \dots \sigma\rangle\rangle|\sigma\alpha\rangle\rangle - |\alpha\sigma\rangle\rangle\big),$$

with nonzero matrix elements:

$$\langle\langle n_\alpha = 1|M_t|n_\beta = 1\rangle\rangle = \delta_{\alpha\beta} - \tilde{E}_{\alpha\beta}/n + \mathcal{O}(1/n^2),$$
$$\tilde{E}_{\alpha\beta} = 2(1 - \langle\langle\sigma\alpha|m_t|\sigma\beta\rangle\rangle).$$

(Note that the "exchange term" $\langle\langle\sigma\alpha|m_t|\beta\sigma\rangle\rangle$ is no longer present). Upon diagonalization of $\tilde{E}_{\alpha\beta}$, the subdominant eigenvalue a_1 is determined, with an identical $1/n$ scaling as found for the symmetric irrep. The possibility that the subdominant eigenvalue lies in this irrep may be removed *a priori* by imposing a natural additional restriction on the random quantum circuit, namely by requiring that the two-qubit gate distribution be invariant under the transformation S that swaps the two-qubits, that is, $\tilde{\mu}(SU) = \tilde{\mu}(US) = \tilde{\mu}(U)$.

From a physical standpoint, it is also interesting to note that the existence of *degenerate* mean-field ground states indicates that $M_t[\mu]$ describes a deformed (or broken-symmetry) phase. For generic $SU(d)$ models in the broken phase, the degeneracy of the ground state manifold is known to be lifted at finite n by tunneling between the mean-field ground states, which induces corrections of order $\exp(-an)$, and hence a gap that closes exponentially in the thermodynamic limit, see *e.g.*, C. M. Newman and L. S. Schulman, J. Math. Phys. **18**, 23 (1977); S. Dusel and J. Vidal, Phys. Rev. B **71**, 224420 (2005) [Ref. [18] in the main text provides additional relevant literature]. Remarkably, *no* such correction can occur in our case because each extremal mean-field state $|\sigma^{(n)}\rangle\rangle$ is an exact eigenoperator of $M_t[\mu]$ for arbitrary finite n, as stressed in the text.

Proof that the leading-order coefficient is non-vanishing

We show here that, for the class of arbitrary permutationally invariant random quantum circuits, the leading-order coefficient a_1 of the $1/n$ term in the spectral gap expansion is nonzero.

Recall that a_1 is given by the minimum eigenvalue of

$$E_{\alpha\beta} = 2(1 - \langle\langle\sigma\alpha|m_t|\sigma\beta\rangle\rangle - \langle\langle\sigma\alpha|m_t|\beta\sigma\rangle\rangle),$$

where $|\alpha\rangle\rangle$ and $|\beta\rangle\rangle$ are operators orthogonal to a permutation $|\sigma\rangle\rangle \in \mathcal{S}_t$. Thus, showing that $a_1 > 0$ is equivalent to showing that $\langle\langle\sigma\alpha|m_t|\sigma\alpha\rangle\rangle + \langle\langle\sigma\alpha|m_t|\alpha\sigma\rangle\rangle < 1$, for any operator $|\alpha\rangle\rangle$ such that $\langle\langle\alpha|\sigma\rangle\rangle = 0$. Let

$$|\psi\rangle\rangle = \frac{1}{\sqrt{2}}(|\sigma\alpha\rangle\rangle + |\alpha\sigma\rangle\rangle).$$

Upon taking the expectation value with respect to m_t, we have

$$\langle\langle\psi|m_t|\psi\rangle\rangle = \tfrac{1}{2}\Big(\langle\langle\sigma\alpha|m_t|\sigma\alpha\rangle\rangle + \langle\langle\sigma\alpha|m_t|\alpha\sigma\rangle\rangle + \langle\langle\alpha\sigma|m_t|\sigma\alpha\rangle\rangle + \langle\langle\alpha\sigma|m_t|\alpha\alpha\rangle\rangle\Big).$$

Since M_t (and hence m_t) is invariant under interchange of any two qubits, $\langle\langle\alpha\sigma|m_t|\sigma\alpha\rangle\rangle = \langle\langle\sigma\alpha|m_t|\alpha\sigma\rangle\rangle$ and $\langle\langle\alpha\sigma|m_t|\alpha\sigma\rangle\rangle = \langle\langle\sigma\alpha|m_t|\sigma\alpha\rangle\rangle$, yielding

$$\langle\langle\psi|m_t|\psi\rangle\rangle = \langle\langle\sigma\alpha|m_t|\sigma\alpha\rangle\rangle + \langle\langle\sigma\alpha|m_t|\alpha\sigma\rangle\rangle.$$

Following from the properties of the invariant subspace $\mathcal{V}_t$ established in the main text, $\langle\langle\psi|m_t|\psi\rangle\rangle = 1$ if and only if the operator $|\psi\rangle\rangle$ is invariant under arbitrary unitary transformations of the form $U^{\otimes t}$ with $U \in U(4)$, given that the corresponding two-qubit gate distribution $\tilde{\mu}(U)$ is universal on $U(4)$. Thus, we must show that there exists a unitary transformation $U \in U(4)$ such that

$$U^{\otimes t}(\sigma \otimes \alpha + \alpha \otimes \sigma)U^{\dagger\otimes t} \neq \sigma \otimes \alpha + \alpha \otimes \sigma.$$

(Recall that, in our notation, we identify $|\alpha\rangle\rangle \equiv \alpha$, and so one). In fact, we may take the permutation $|\sigma\rangle\rangle$ to be the identity $|I\rangle\rangle$ without loss of generality. This follows upon noting that

$$\langle\langle\psi|m_t|\psi\rangle\rangle = \int d\tilde{\mu}(U)\mathrm{tr}[\psi^\dagger U^{\otimes t}\psi U^{\dagger\otimes t}].$$

Since $\sigma U^{\otimes t} = U^{\otimes t}\sigma$ for all $U \in U(4)$, $\psi^\dagger \sigma U^{\otimes t}\sigma^\dagger \psi U^{\dagger\otimes t} = \psi^\dagger U^{\otimes t}\psi U^{\dagger\otimes t}$. Thus, $\sigma\otimes\alpha+\alpha\otimes\sigma$ has the same expectation value as $I\otimes\tilde{\alpha}+\tilde{\alpha}\otimes I$, where $\tilde{\alpha} = \sigma^\dagger\alpha$.

Any operator $|\tilde{\alpha}\rangle\rangle$ orthogonal to the identity may be expanded $\tilde{\alpha} = \sum_\nu c_\nu \sigma^1_{\nu_1}\dots\sigma^t_{\nu_t}$, where $\nu = (\nu_1,\dots,\nu_t)$, and $\nu_i \in \{0,1,2,3\}$, with $\sigma_0 = I$, $\sigma_1 = \sigma_x$, $\sigma_2 = \sigma_y$, $\sigma_3 = \sigma_z$, and the sum ranges over all possible strings ν except the one where $\nu_i = 0\ \forall i$. Thus, $\tilde{\alpha}\otimes I = \sum_\nu c_\nu \sigma^1_{\nu_1}\otimes I^1\dots\sigma^t_{\nu_t}\otimes I^t$. Now, under $U = \exp(\frac{\pi}{4}i\sigma_3\otimes\sigma_3)$, the following transformations hold for Pauli operators:

$$\begin{aligned}
\sigma_1\otimes I &\mapsto -\sigma_2\otimes\sigma_3,\\
\sigma_2\otimes I &\mapsto \sigma_1\otimes\sigma_3,\\
\sigma_3\otimes I &\mapsto \sigma_3\otimes I,\\
I\otimes\sigma_1 &\mapsto -\sigma_3\otimes\sigma_2,\\
I\otimes\sigma_2 &\mapsto \sigma_3\otimes\sigma_1,\\
I\otimes\sigma_3 &\mapsto I\otimes\sigma_3.
\end{aligned}$$

Thus, for any $|\tilde{\alpha}\rangle\rangle$ with support on a Pauli string such that $\nu_i = 1$ or 2 for some i, there are terms in the expansion of $U^{\otimes t}(I\otimes\tilde{\alpha}+\tilde{\alpha}\otimes I)U^{\dagger\otimes t}$ which contain factors of the form $\sigma_2\otimes\sigma_3$, $\sigma_3\otimes\sigma_2$, $\sigma_1\otimes\sigma_3$, and $\sigma_3\otimes\sigma_1$. Since there are no such term in the expansion of $I\otimes\tilde{\alpha}+\tilde{\alpha}\otimes I$, it follows that $I\otimes\tilde{\alpha}+\tilde{\alpha}\otimes I$ is *not* invariant under $(\exp(\frac{\pi}{4}i\sigma_3\otimes\sigma_3))^{\otimes t}$. Similarly, if $|\tilde{\alpha}\rangle\rangle$ has support on any Pauli string such that $\nu_i = 3$ or 2 for some i, then $I\otimes\tilde{\alpha}+\tilde{\alpha}\otimes I$ is not invariant under $(\exp(\frac{\pi}{4}i\sigma_1\otimes\sigma_1))^{\otimes t}$. Since $|\tilde{\alpha}\rangle\rangle$ must belong to one of these two cases, the proof is complete. □

Proof that the leading-order coefficient is t-independent

We next show that, under the additional assumption that $\tilde{\mu}(U)$ is invariant under the subgroup $U(2)\times U(2)\subset U(4)$ of local unitary transformations on the two target qubits, the leading order coefficient a_1 of the $1/n$ expansion does not depend on t.

Recall that a_1 is determined by the maximum value of $\langle\langle\sigma\omega|m_t|\sigma\omega\rangle\rangle + \langle\langle\sigma\omega|m_t|\omega\sigma\rangle\rangle$, where $\sigma\in\mathcal{S}_t$ and $|\omega\rangle\rangle$ is a $U(2)$ invariant which is orthogonal to $|\sigma\rangle\rangle$. As shown previously, we may take $|\sigma\rangle\rangle$ to be the identity without loss of generality. Now, any operator orthogonal to the identity may be expanded as $\omega = \sum_\nu c_\nu\sigma^1_{\nu_1}\dots\sigma^t_{\nu_t}$ where, as before, $\nu = (\nu_1,\dots,\nu_t)$, and $\nu_i\in\{0,1,2,3\}$, with $\sigma_0 = I$, $\sigma_1=\sigma_x$, $\sigma_2=\sigma_y$, $\sigma_3=\sigma_z$, and the sum ranges over all possible strings ν except the one where $\nu_i = 0\ \forall i$.

The first step is to show that the expectation value $\langle\langle I\omega|U^{\otimes t,t}|I\omega\rangle\rangle$ for any $U\in U(4)$ may be written as a symmetric polynomial of the form

$$\langle\langle I\omega|U^{\otimes t,t}|I\omega\rangle\rangle = \sum_{2\le p_1+p_2+p_3\le t} w_{\vec{p}}\, x^{p_1}y^{p_2}z^{p_3}, \qquad (4)$$

where x, y, z are real numbers in $[-1,1]$ which depend only on U, and $w_{\vec{p}}$ are positive coefficients which depend only on $|\omega\rangle\rangle$, with $\vec{p} = (p_1,p_2,p_3)$ and p_i being non-negative integers subject to $2\le p_1+p_2+p_3\le t$.

To establish Eq. (4) above, we exploit the fact that an arbitrary element of $U(4)$ may be written in the canonical decomposition form $U = U_1\otimes U_2\,U(q,r,s)\,U_1'\otimes U_2'$, where U_1, U_1', U_2, U_2' act locally on either of two qubits and $U(q,r,s) = \exp\{i(q\sigma_1\otimes\sigma_1+r\sigma_2\otimes\sigma_2+s\sigma_3\otimes\sigma_3)\}$ [see *e.g.* B. Kraus and J. I. Cirac, Phys. Rev. A **63**, 062309 (2001)]. Since $|\omega\rangle\rangle$ is a $U(2)$ invariant, it then suffices to consider the action of $U(q,r,s)$. Direct calculation shows that under $U(q,r,s)$, the following transformations are obeyed by Pauli operators:

$$\begin{aligned}
I\otimes\sigma_1 &\mapsto r_1s_1\ I\otimes\sigma_1 + r_2s_1\ \sigma_2\otimes\sigma_3\\
&\quad - r_1s_2\ \sigma_3\otimes\sigma_2 + r_2s_2\ \sigma_1\otimes I, &(5)\\
I\otimes\sigma_2 &\mapsto s_1q_1\ I\otimes\sigma_2 + s_2q_1\ \sigma_3\otimes\sigma_1\\
&\quad - s_1q_2\ \sigma_1\otimes\sigma_3 + s_2q_2\ \sigma_2\otimes I, &(6)\\
I\otimes\sigma_3 &\mapsto q_1r_1\ I\otimes\sigma_3 + q_2r_1\ \sigma_1\otimes\sigma_2\\
&\quad - q_1r_2\ \sigma_2\otimes\sigma_1 + q_2r_2\ \sigma_3\otimes I, &(7)
\end{aligned}$$

where $q_1 = \cos(2q)$, $q_2 = \sin(2q)$, and similar expressions hold for r_1, r_2, and s_1, s_2, respectively.

The idea is now to evaluate $U^{\otimes t,t}|I\omega\rangle\rangle$ term by term in the expansion for $|\omega\rangle\rangle$, that is, we evaluate

$$\begin{aligned}
U^{\otimes t}(I\otimes\omega)\,U^{\dagger\otimes t} &= \sum_\nu c_\nu U^{\otimes t}\,(I^1\otimes\sigma^1_{\nu_1}\dots I^t\otimes\sigma^t_{\nu_t})\,U^{\dagger\otimes t}\\
&= \sum_\nu c_\nu \bigotimes_{i=1}^{t} U(I^i\otimes\sigma^i_{\nu_i})U^\dagger,
\end{aligned}$$

where now the transformation rules in Eq. (5)-(7) may be applied to each of the t factors independently. Computing the matrix element $\langle\langle I\omega|U^{\otimes t,t}|I\omega\rangle\rangle$, there is a contribution of the form $|c_\nu|^2x^{p_1}y^{p_2}z^{p_3}$, arising from each of the terms $c_\nu I^1\otimes\sigma^1_{\nu_1}\dots I^t\otimes\sigma^t_{\nu_t}$, where $x = r_1s_1$, $y = s_1q_1$, $z = q_1r_1$, and p_1, p_2, p_3 are the number of instances where $\nu_i = 1,2,3$, respectively. Summing over all terms in the expansion for $|\omega\rangle\rangle$ finally results in a polynomial of the form stipulated in Eq. (4), with $w_{\vec{p}} = \sum_\nu |c_\nu|^2$ determined by the sum over all strings ν that share the same $\vec{p}$-vector. That the polynomial is symmetric under the interchange of x, y, and z follows from the invariance of $|\omega\rangle\rangle$ under $U(2)$. Note that by construction, x, y, and z are bounded between $[-1,1]$.

Let the degree of a Pauli string be the number of instances where $\nu_i\ne 0$. Since, under $U^{\otimes t}$ with $U\in U(2)$, a Pauli string can only be mapped to a Pauli string of equal degree, it follows that any $U(2)$ invariant whose expansion contains terms of differing degree can be written as a linear combination of $U(2)$ invariants each containing only terms of equal degree. For $t = 1$, the only $U(2)$ invariant is the identity. For $t = 2$, there is exactly one $U(2)$ invariant orthogonal to the identity, namely, $\omega = \frac{1}{\sqrt{3}}(\sigma^1_1\sigma^2_1+\sigma^1_2\sigma^2_2+\sigma^1_3\sigma^2_3)$. Consequently, no $U(2)$ invariant contains a term of degree 1, and the only degree-2 terms a $U(2)$ invariant may contain are linear combinations of the form $\sigma^i_1\sigma^j_1+\sigma^i_2\sigma^j_2+\sigma^i_3\sigma^j_3$. Thus, for a monomial occurring in $\sum_{\vec{p}} w_{\vec{p}}x^{p_1}y^{p_2}z^{p_3}$, $2\le p_1+p_2+p_2\le t$,

and if $p_1 + p_2 + p_3 = 2$, then exactly one of p_1, p_2, or $p_3 = 2$.

The next step to establish the claimed result is to show that $\sum_{\vec{p}} w_{\vec{p}} x^{p_1} y^{p_2} z^{p_3} \leq \frac{1}{3}(x^2 + y^2 + z^2)$, where the right hand side is the polynomial corresponding to $\langle\langle I\omega_2 | U^{\otimes t,t} | I\omega_2 \rangle\rangle$, where $|\omega_2\rangle\rangle$ is any degree-2 $U(2)$ invariant. To show this we first show that the average over each set of monomials $x^{p_1} y^{p_2} z^{p_3}$ defined by a set of integers $p \geq p' \geq p''$ distributed in every distinct way to p_1, p_2, and p_3, is less than or equal to $\frac{1}{3}(x^2 + y^2 + z^2)$. There are two cases to consider:

(i) If $p \geq 2$, then from $|x|, |y|, |z| \leq 1$, it follows that $x^p \frac{1}{2}(y^{p'} z^{p''} + y^{p''} z^{p'}) \leq x^2$, $y^p \frac{1}{2}(z^{p'} x^{p''} + z^{p''} x^{p'}) \leq y^2$, and $z^p \frac{1}{2}(x^{p'} y^{p''} + x^{p''} y^{p'}) \leq z^2$. Thus, the average of the left hand side of each inequality, which is the average over the desired set of monomials, must be less than or equal to the average of the right hand sides, which is $\frac{1}{3}(x^2 + y^2 + z^2)$.

(ii) If $p = p' = p'' = 1$, then using $x = r_1 s_1$, $y = s_1 q_1$ and $z = q_1 r_1$, $xyz \leq \frac{1}{3}(x^2 + y^2 + z^2)$ can be written $q_1^2 r_1^2 s_1^2 \leq \frac{1}{3}(r_1^2 s_1^2 + s_1^2 q_1^2 + q_1^2 r_1^2)$, which follows from $q_1^2 r_1^2 s_1^2 \leq r_1^2 s_1^2, s_1^2 q_1^2, q_1^2 r_1^2$.

Since $\sum_{\vec{p}} w_{\vec{p}} x^{p_1} y^{p_2} z^{p_3}$ is a weighted average of the above monomial averages, each of which is less than or equal to $\frac{1}{3}(x^2 + y^2 + z^2)$, it follows that $\sum_{\vec{p}} w_{\vec{p}} x^{p_1} y^{p_2} z^{p_3} \leq \frac{1}{3}(x^2 + y^2 + z^2)$.

Finally, the steps described above can be applied to the exchange term $\langle\langle I\omega | U^{\otimes t,t} | \omega I \rangle\rangle$, resulting in $\langle\langle I\omega | U^{\otimes t,t} | \omega I \rangle\rangle \leq \frac{1}{3}(x^2 + y^2 + z^2)$, where $x = b_2 c_2$, $y = a_2 c_2$, $z = a_2 b_2$ for any $U \in U(4)$. Since these inequalities hold for every $U \in U(4)$, it follows that

$$\begin{aligned} \langle\langle I\omega | m_t | I\omega \rangle\rangle \;&+\; \langle\langle I\omega | m_t | \omega I \rangle\rangle \\ &\leq\; \langle\langle I\omega_2 | m_t | I\omega_2 \rangle\rangle + \langle\langle I\omega_2 | m_t | \omega_2 I \rangle\rangle, \end{aligned}$$

where $|\omega_2\rangle\rangle$ is any degree-2 $U(2)$ invariant. Since $\langle\langle I\omega_2 | U^{\otimes t,t} | I\omega_2 \rangle\rangle = \frac{1}{3}(x^2 + y^2 + z^2)$ (and the equivalent expression for $\langle\langle I\omega_2 | U^{\otimes t,t} | \omega_2 I \rangle\rangle$) holds for every degree-2 $U(2)$ invariant, and the expression does not depend on t, it follows that the maximum of $\langle\langle I\omega | m_t | I\omega \rangle\rangle + \langle\langle I\omega | m_t | \omega I \rangle\rangle$ over all $|\omega\rangle\rangle$ such that $\langle\langle \omega | I \rangle\rangle = 0$ is given by $\langle\langle I\omega_2 | m_2 | I\omega_2 \rangle\rangle + \langle\langle I\omega_2 | m_2 | \omega_2 I \rangle\rangle$. This concludes the proof. $\square$